h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Hochschule Darmstadt

- Fachbereich Informatik -

Ein Beispieltitel für eine Thesis der mehrere Zeilen umfasst und seriös wirkt

Abschlussarbeit zur Erlangung des akademischen Grades
Bachelor of Science (B.Sc.)

vorgelegt von

John Doe

7. Februar 2017

Referent:	Prof. Dr. Max Mustermann
Korreferent:	Prof. Dr. Jane Example

Abstract (Deutsch)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln. Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Abstract

This is analogous to the German Abstract.

Erklärung

Ich versichere hiermit, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die im Literaturverzeichnis angegebenen Quellen benutzt habe. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder noch nicht veröffentlichten Quellen entnommen sind, sind als solche kenntlich gemacht. Die Zeichnungen oder Abbildungen in dieser Arbeit sind von mir selbst erstellt worden oder mit einem entsprechenden Quellennachweis versehen. Diese Arbeit ist in gleicher oder ähnlicher Form noch bei keiner anderen Prüfungsbehörde eingereicht worden.

Darmstadt, den 7. Februar 2017

John Doe: .....

Inhaltsverzeichnis

Abbildungsverzeichnis

Listings

Tabellenverzeichnis

Akronyme

API	Application Programming Interface
BC	BouncyCastle
BLOB	Binary Large Object
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
CSP	Certification Service Provider
E2E	Ende-zu-Ende
GPG	GNU Privacy Guard
GPL	GNU Public License
GZHK	Größte Zusammenhangskomponente
HSM	Hardware Security Module
ID	Identifikationsnummer
IETF	Internet Engineering Task Force
JSON	Javascript Object Notation
PGP	Pretty Good Privacy
PKC	Public Key Kryptographie
PKI	Public Key Infrastructure
RA	Registration Authority
SFTP	Secure File Transfer Protocol
UID	User ID
UTC	Coordinated Universal Time
VV	Volksverschlüsselung
WoT	Web of Trust

Danksagung

Ich danke meinen Prüfern und Betreuern, Herrn Prof. Dr. Max Baum und Prof. Dr. Jane Example, für...

Kapitel 1

Einführung

> Benutze paragraphs wenn, wenn sections zu viel Trennung zu viel sind aber du eine Gliederung deutlich machen willst.

Einordnung Ende-zu-Ende (E2E) E-Mail Verschlüsselung gewann spätestens mit den Snowden-Leaks 2013 auch außerhalb der IT-Szene an Bedeutung.

Notwendigkeit [Bur15] zeigt, dass die Verbreitung der Transportverschlüsselung zwischen den E-Mail-Servern und zum Nutzer zunimmt.

> Nutzung von Fußnoten und Acrfull

Ende-zu-Ende (E2E)-verschlüsselt[1]

Marktlücke Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

[1] Repräsentative Umfrage von Bitkom: 15% der Nutzer verschlüsselten in 2015 E-Mails teilweise [Bit16]

> Benutzung von
> emph für gewisse Eigennamen

Arbeitsumfeld Verantwortlich für das Projekt ist die Abteilung *Cloud Computing and Identity & Privacy* des SIT.

Der Autor war von Februar bis Juni 2016 Teil des Teams und entwickelte dort die OpenPGP-Erweiterung, der dem Projekt zugrunde liegenden PKI.

Kapitel 2

Problemstellung

Liste mit Punkten die die Lösung erfüllen soll:

1. Erster Listenpunkt, Stufe 1
2. Zweiter Listenpunkt, Stufe 1
3. Dritter Listenpunkt, Stufe 1
4. Vierter Listenpunkt, Stufe 1
5. Fünfter Listenpunkt, Stufe 1
6. Sechster Listenpunkt, Stufe 1
7. Siebter Listenpunkt, Stufe 1
8. Achter Listenpunkt, Stufe 1
9. Neunter Listenpunkt, Stufe 1
10. Zehnter Listenpunkt, Stufe 1

Kapitel 3

Grundlagen

S/MIME ist standardisiertes Format zur Verschlüsselung von E-Mails und setzt X.509 Zertifikate ein. S/MIME und OpenPGP sind inkompatibel (Absatz vgl. [Sch13, S. 667f]).

Abb. 3.1 zeigt die beschriebenen drei bzw. vier Akteure der Kommunikation.

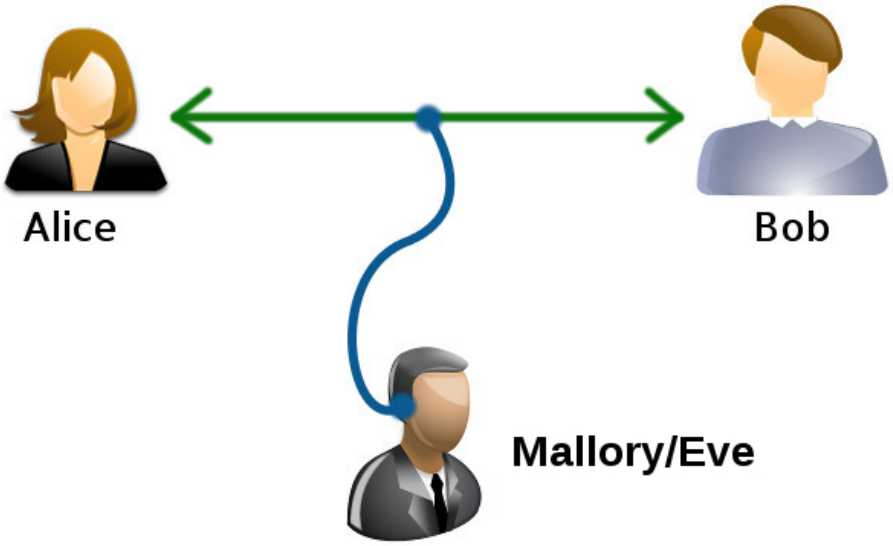

Abbildung 3.1: Vorstellung von Alice, Bob und Eve
Quelle: Ursprünglich von Didia (Own work) [CC BY-SA 4.0 (http://creativecommons.org/licenses/by-sa/4.0)], via Wikimedia Commons mit Änderung des Bezeichnung Mallory [Did]

3.1 OpenPGP

> Cite mit Seitenangabe

Es ist eines der am weitesten verbreiteten Werkzeuge zur E-Mail- und Dateiverschlüsselung ([Ann11, S. 995]).

Cite eines RFC

1998 standardisierte die OpenPGP Working Group PGP bei der Internet Engineering Task Force (IETF) als „OpenPGP Message Format“ in [RFC4880].

vref, smartref und autoref im Vergleich

Kapitel 4 auf Seite 9
Kapitel 4, „Arbeitstitel-oder -thema (Lösung)“, auf Seite 9
Kapitel 4

cite mit mehreren Quellen

[Ben01; Kre99; Way; Fre])

benutzung von verb

In der vorliegenden Arbeit wird diese Software für Untersuchungen und zu Demonstationszwecken in den Versionen `gpg 1.4.18` bzw. `gpg2 2.0.28` verwendet

Eine Referenz auf eine Zeile in einem Listing

Die verwendeten Subpaket-Klassen beschränken sich lediglich auf 2 (Datum) und 29 (Grund des Widerrufs) in Zeile 4f.

LISTING 3.1: Ein PGP-Paket

```
1 :signature packet: algo 1, keyid 959FEB541D9FCFE5
2 version 4, created 1462880534, md5len 0, sigclass 0x30
3 digest algo 2, begin of digest b3 50
4 hashed subpkt 2 len 4 (sig created 2016-05-10)
5 hashed subpkt 29 len 15 (revocation reason 0x00 (this is a
     test))
6 subpkt 16 len 8 (issuer key ID 959FEB541D9FCFE5)
7 data: [2046 bits]
```

Eine in der Breite beschränkte Grafik (0.8)

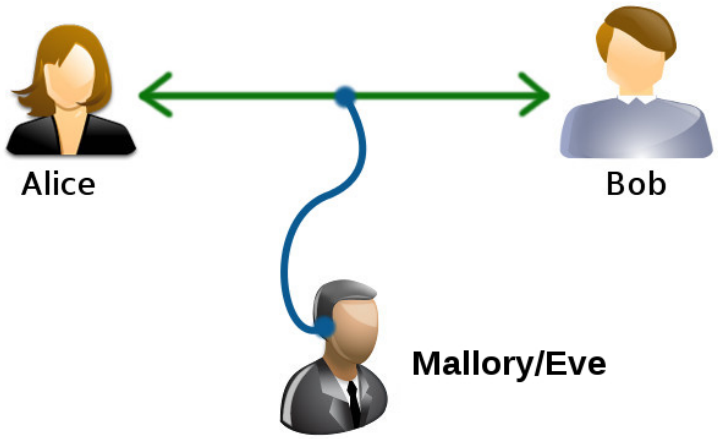

Abbildung 3.2:
Vorstellung von Alice, Bob und Eve
Quelle: Ursprünglich von Dia (Own work) [CC BY-SA 4.0 (http://creativecommons.org/licenses/by-sa/4.0)], via Wikimedia Commons mit Änderung des Bezeichnung Mallory [Did]

Eine in der Höhe beschränkte Grafik (0.6); **Zeigen wie man subscripts in Captions unterbringt**

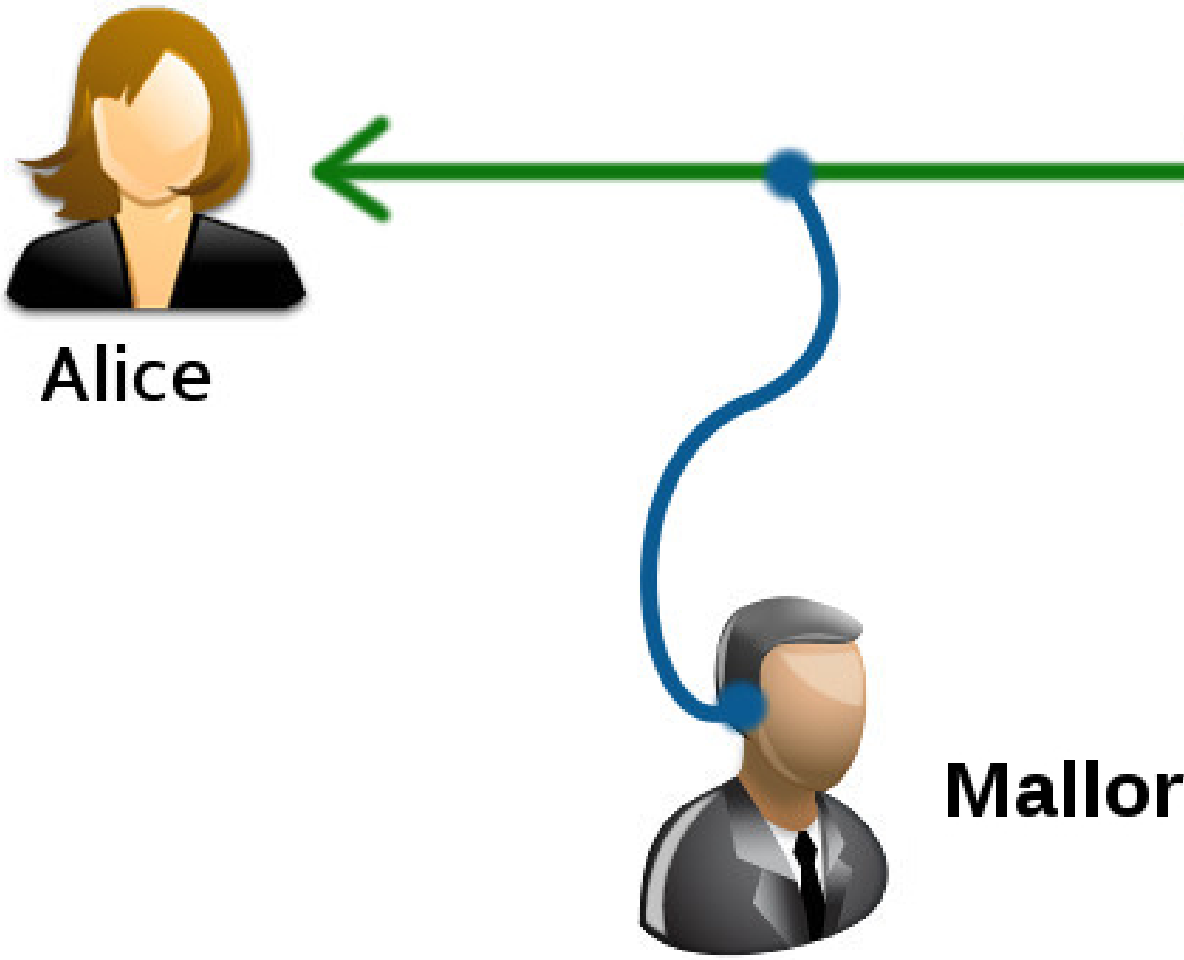

Abbildung 3.3: Subscript test $Variable_{\text{subscript}}$
Quelle: Ursprünglich von Didia (Own work) [CC BY-SA 4.0 (http://creativecommons.org/licenses/by-sa/4.0)], via Wikimedia Commons mit Änderung des Bezeichnung Mallory [Did]

> Eingerückter Text

1. **Sitzungs-ID** Lorem ipsum dolor sit amet

2. **Authentifizierung** Lorem ipsum dolor sit amet

3. **Verifikation** Lorem ipsum dolor sit amet

Ein Beispielaufruf des Uploads zeigt Listing 3.2.

> Inlining von Latex-Kommandos in Listings (z.B. zum Fett-drucken) (escapeinside)

LISTING 3.2: Beispielanfrage zum Upload eines Keys

```
1 POST /certs/?pid=flJvlYAH...CKQZusIT&cert_type=encr HTTP/1.1
2 [...]
3 --01ead4a5-7a67-4703-ad02-589886e00923
4 [...]
5 --01ead4a5-7a67-4703-ad02-589886e00923
```

Kapitel 4

Arbeitstitel-oder -thema (Lösung)

In diesem Kapitel wird die eigene Arbeit beschrieben, ein Konzept, Implementierung, Messergebnisse oder ähnliches.

„Sonderzeichen“ im Math-mode:
$Länge_{signatur} <= N$

Zentrieren eines Texts

Eine typische UID sieht wie folgt aus:

```
Max Mustermann (beruflich) <mm@example.com>
```

Eine einfache Tabelle mit hervorgehobenen Boxen

Tabelle 4.1: Akzeptierte Reihenfolgen der Namensbestandteile einer UID

				Beispiel
1	Titel	Vornamen	Nachnamen	Dr. Max Baum
2	Titel	Nachnamen	Vornamen	Dr. h. c. Ban Ki-moon
3		Vornamen	Nachnamen	Max Baum
4		Nachnamen	Vornamen	Ban Ki-moon
5		Nachnamen ,	Vornamen	Baum, Max

Kryptographische- und Sicherheits-Eigenschaften

Wörtliches Zitieren, zweisprachig

„OpenPGP implementations MUST create keys with version 4 format. V3 keys are deprecated;“ [RFC4880, S.40]
Deutsch: *OpenPGP Implementierungen müssen [zwingend] Schlüssel im Format der Version 4 erzeugen. Schlüssel der Version 3 sind veraltet;*

Eine Description, genutzt zum Auflisten einer key-value Liste mit hervorgehobenem key

OK
`Prof. Dr. Frank Emil Schuster <fes@example.com>`

OK Kein Titel
`Frank Emil Schuster <fes@example.com>`

Fehler Unvollständiger Vorname
`Prof. Dr. Frank Schuster <fes@example.com>`

Fehler Falsche E-Mail-Adresse
`Prof. Dr. Frank Emil Schuster <NOBODY@example.com>`

OK Kommentare werden gefiltert
`(foo)Frank Emil Schu()ster (foo) <fes@exampl(foo)e.com>`

Eine Description, mit minimierten Zeilenzwischenräumen

≈ **3s** Authentifikation und Stellung des Zertifizierungsauftrags
≈ **2s bis 48s** Warten auf CA und XML-Austausch
≈ **300ms** Herunterladen des Zertifikats und Senden eines Sperrauftrags

Eine Komplexe, mehrzeilige Tabelle

TABELLE 4.2: Überblick über Optionen der Publikation von Zertifikatsdaten

Option	**Verteilung**	**Umfang veröffentlichter Daten** [a]	**Auffindbarkeit**
1	Manuell	Keine	Keine[b]
2	Keyserver	Public-Key-Material (PGPCA-)Signatur	per Key-ID[c]
3	Keyserver	Public-Key-Material User-ID + Selbst-Signatur (PGPCA-)Signatur	per Key-ID, E-Mail Adresse, Namen

[a] Hervorgehobene Box steht für OpenPGP-Paket
[b] solange keine Sperrung vorliegt
[c] keine Preisgabe von personenbezogenen Daten

Kapitel 5

Implementierung

Was wurde vom Konzept implementiert, was fehlt noch, was ist unvollständig?

Vollständig Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Unvollständig Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Ausstehend Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben,

sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Kapitel 6

Auswertung

6.1 Überprüfung der Anforderungserfüllung

1. **Anforderung 1**
   Anforderung 1 wurde erfüllt, weil... So wurde es gelöst (kurz)
2. **Anforderung 2**
   Anforderung 2 wurde erfüllt, weil... So wurde es gelöst (kurz)

Kapitel 7

Zusammenfassung

Was leistet die Lösung, was wurde gelöst, welche Kritik gibt es, was hat diese Arbeit erreicht für die Forschung und andere Bereiche? Welche Erkenntnisse gewann der/dir Autor*in beim Schreiben?

Kapitel 8

Ausblick

Was wird mit dem Thema weiter passieren, sind Trends abzusehen, wird die Relevanz des Themas bleiben?

8.1 Weiterentwicklung

Welche Weiterentwicklung wird/muss passieren?

8.2 Forschung

Welche Forschungsbereiche/-Fragen wurden entdeckt, könnten in Zukunft bearbeitet werden?

Anhang A

Listings

A.1 Programmablauf Hello World

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Listing A.1: Code Fragment of Hello World Class

```
1 /**
2 * The HelloWorldApp class implements an application
    that
3 * simply prints "Hello World!" to standard output.
4 */
5 class HelloWorldApp {
6   public static void main(String[] args) {
7   System.out.println("Hello World!"); // Display the
      string.
8   }
9 }
```

Literatur

[Alb15] Klaus-Dieter Wolfenstetter (auth.) Albrecht Beutelspacher Jörg Schwenk. *Moderne Verfahren der Kryptographie: Von RSA zu Zero-Knowledge*. 8. Aufl. Wiesbaden: Springer Spektrum, 2015. ISBN: 978-3-8348-1927-7.

[Ang] Julia Angwin. *The World's Email Encryption Software Relies on One Guy, Who is Going Broke*. URL: https://www.propublica.org/article/the-worlds-email-encryption-software-relies-on-one-guy-who-is-going-broke (zuletzt besucht am: 16. 12. 2016).

[Ann11] Sushil Jajodia (eds.) Anne Canteaut Prof. (auth.) Henk C. A. van Tilborg. *Encyclopedia of Cryptography and Security*. 2. Aufl. New York: Springer US, 2011. ISBN: 978-1-4419-5905-8.

[Bar+15] Alessandro Barenghi u. a. „Computer Security – ESORICS 2015: 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I". In: Hrsg. von Günther Pernul, Peter Y A Ryan und Edgar Weippl. Cham: Springer International Publishing, 2015. Kap. Challenging the Trustworthiness of PGP: Is the Web-of-Trust Tear-Proof?, S. 429–446. ISBN: 978-3-319-24174-6. DOI: 10.1007/978-3-319-24174-6_22. URL: http://dx.doi.org/10.1007/978-3-319-24174-6_22.

[Ben01] Ralf Bendrath. *PGP - die ersten zehn Jahre*. 19. März 2001. URL: https://www.heise.de/tp/features/PGP-die-ersten-zehn-Jahre-3447927.html (zuletzt besucht am: 21. 16. 2016).

[Bit16] Bitkom. *Verschlüsselung von E-Mails kommt nur langsam voran*. 21. Jan. 2016. URL: https://www.bitkom.org/Presse/Presseinformation/Verschluesselung-von-E-Mails-kommt-nur-langsam-voran.html (zuletzt besucht am: 14. 11. 2016).

[Bou] BouncyCastle Autoren. *Support and FIPS FAQ*. URL: https://www.cryptoworkshop.com/support_faq.html (zuletzt besucht am: 21. 12. 2016).

[BR15] Elaine Barker und Allen Roginsky. *NIST Special Publication 800-131A*. 2015. URL: http://dx.doi.org/10.6028/NIST.SP.800-131Ar1 (zuletzt besucht am: 03. 12. 2016).

[Bun] Bundesrepublik Deutschland. *Bundesdatenschutzgesetz*. URL: https://www.gesetze-im-internet.de/bdsg_1990/__3.html (zuletzt besucht am: 15. 12. 2016).

[Bun15] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen. *Algorithmenkatalog 2016*. 9. Dez. 2015. URL: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2016Algorithmenkatalog.pdf?__blob=publicationFile&v=1 (zuletzt besucht am: 15. 11. 2016).

[Bur15] Elie Bursztein. *New Research: Encouraging trends and emerging threats in email security*. Nov. 2015. URL: https://security.googleblog.com/2015/11/new-research-encouraging-trends-and.html (zuletzt besucht am: 14. 11. 2016).

[CBH02] Srdjan Capkun, Levente Buttyan und Jean-Pierre Hubaux. „Small Worlds in Security Systems: an Analysis of the PGP Certificate Graph“. In: *In Proceedings of The ACM New Security Paradigms Workshop*. ACM Press, 2002, S. 28–35.

[Coe] Everaldo Coelho. *Crystal Clear*. URL: https://commons.wikimedia.org/wiki/Crystal_Clear (zuletzt besucht am: 09. 01. 2017).

[Did] Didia. URL: https://commons.wikimedia.org/wiki/File%3AAlice-bob-mallory.jpg (zuletzt besucht am: 16. 12. 2016).

[Ela] National Institute of Standards and Technology NIST Elaine Barker. *Recommendation for Key Management*. URL: http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4 (zuletzt besucht am: 02. 01. 2017).

[Eur] Europäische Union. *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES*. URL: http://eur-lex.europa.eu/legal-content/DE/

TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.DEU (zuletzt besucht am: 14. 11. 2016).

[Fie00] Roy Thomas Fielding. „Architectural styles and the design of network-based software architectures“. Diss. University of California, Irvine, 2000. URL: http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm (zuletzt besucht am: 19. 12. 2016).

[Fre] Free Software Foundation. URL: https://git.gnupg.org/cgi-bin/gitweb.cgi?p=gnupg.git;a=blob_plain;f=COPYING;hb=refs/heads/master (zuletzt besucht am: 16. 12. 2016).

[Gil] David Leon Gil. *OpenPGPv4 long keyid collision test cases?* URL: https://www.ietf.org/mail-archive/web/openpgp/current/msg07195.html (zuletzt besucht am: 07. 12. 2016).

[GNO] GNOME icon artists. *GNOME Desktop icons*. URL: https://commons.wikimedia.org/wiki/GNOME_Desktop_icons (zuletzt besucht am: 16. 12. 2016).

[Gnua] GnuPG Autoren. *gpg manpage*. URL: https://www.gnupg.org/gph/de/manual/r1023.html (zuletzt besucht am: 16. 12. 2016).

[Gnub] GnuPG Autoren. *Release Notes*. URL: https://gnupg.org/download/release_notes.html (zuletzt besucht am: 16. 12. 2016).

[Gnuc] GnuPG Project. *GnuPG FAQ*. URL: https://www.gnupg.org/faq/gnupg-faq.html (zuletzt besucht am: 14. 11. 2016).

[Has16] Tankred Hase. *Mailvelope Keyserver Readme*. 2016. URL: https://github.com/mailvelope/keyserver (zuletzt besucht am: 23. 11. 2016).

[Hei] Heise Verlag. *Heise Krypto-Kampagne FAQ*. URL: http://heise.de/-473427 (zuletzt besucht am: 18. 11. 2016).

[Hol14] Ralph Holz. „Empirical analysis of Public Key Infrastructures and investigation of improvements“. Diss. 2014. URL: http://www.net.in.tum.de/fileadmin/bibtex/publications/theses/NET-2014-05-1.pdf (zuletzt besucht am: 20. 12. 2016).

[JMV14] Don Johnson, Alfred Menezes und Scott Vanstone. „The Elliptic Curve Digital Signature Algorithm (ECDSA)“. In: *International Journal of Information Security* 1.1 (2014), S. 36–63. ISSN: 1615-5262. DOI: 10.1007/s102070100002. URL: http://dx.doi.org/10.1007/s102070100002.

[Jos] Oskari Saarenmaa Joseph Galbraith. *SSH File Transfer Protocol*. URL: https://tools.ietf.org/html/draft-ietf-secsh-filexfer-13 (zuletzt besucht am: 05. 01. 2017).

[Kre99] Stefan Krempl. *Bundesregierung fördert Open Source*. 15. Nov. 1999. URL: https://www.heise.de/tp/features/Bundesregierung-foerdert-Open-Source-3444768.html (zuletzt besucht am: 21. 16. 2016).

[Mer] Merlin2525. URL: https://openclipart.org/detail/192936/server-remix-1g (zuletzt besucht am: 16. 12. 2016).

[Mil67] Stanley Milgram. „The Small World Problem“. In: *Psychology Today* 1.1 (1967), S. 61–67. URL: http://snap.stanford.edu/class/cs224w-readings/milgram67smallworld.pdf.

[MyS] MySQL Autoren. *MySQL 5.6 Data Storage Requirements*. URL: https://dev.mysql.com/doc/refman/5.6/en/storage-requirements.html (zuletzt besucht am: 14. 11. 2016).

[RFC2505] G. Lindberg. *Anti-Spam Recommendations for SMTP MTAs*. RFC 2505 (Best Current Practice). Internet Engineering Task Force, Feb. 1999. URL: http://www.ietf.org/rfc/rfc2505.txt.

[RFC2822] P. Resnick. *Internet Message Format*. RFC 2822 (Proposed Standard). Obsoleted by RFC 5322, updated by RFCs 5335, 5336. Internet Engineering Task Force, Apr. 2001. URL: http://www.ietf.org/rfc/rfc2822.txt.

[RFC4251] T. Ylonen und C. Lonvick. *The Secure Shell (SSH) Protocol Architecture*. RFC 4251 (Proposed Standard). Internet Engineering Task Force, Jan. 2006. URL: http://www.ietf.org/rfc/rfc4251.txt.

[RFC4880] J. Callas u. a. *OpenPGP Message Format*. RFC 4880 (Proposed Standard). Updated by RFC 5581. Internet Engineering Task Force, Nov. 2007. URL: http://www.ietf.org/rfc/rfc4880.txt.

[RFC5280] D. Cooper u. a. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280 (Proposed Standard). Updated by RFC 6818. Internet Engineering Task Force, Mai 2008. URL: http://www.ietf.org/rfc/rfc5280.txt.

[Sch13] Klaus Schmeh. *Kryptografie. Verfahren, Protokolle, Infrastrukturen*. 5. Aufl. Heidelberg: dpunkt.verlag, 2013. ISBN: 978-3-86490-015-0.

[Sha] David Shaw. *The OpenPGP HTTP Keyserver Protocol (HKP)*. URL: https://tools.ietf.org/html/draft-shaw-openpgp-hkp-00 (zuletzt besucht am: 05. 01. 2017).

[Sic09] Bundesamt für Sicherheit in der Informationstechnik BSI. *BSI-Position zu X.509-Zertifikaten mit Signatur auf Basis des MD5-Algorithmus*. 8. Jan. 2009. URL: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2009/080109x509zert.html (zuletzt besucht am: 15. 11. 2016).

[Sic16] Bundesamt für Sicherheit in der Informationstechnik BSI. *Technische Richtlinie – Kryptographische Verfahren: Empfehlungen und Schlusselllängen*. 2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=2 (zuletzt besucht am: 15. 11. 2016).

[Sie] Ben Siegler. *Auf der Suche nach der Volksverschlüsselung*. URL: https://netzpolitik.org/2016/auf-der-suche-nach-der-volksverschluesselung/ (zuletzt besucht am: 16. 12. 2016).

[Stö] Christian Stöcker. *Die drei Haken der "Volksverschlüsselung"*. URL: http://www.spiegel.de/netzwelt/netzpolitik/volksverschluesselung-gute-idee-mit-vielen-haken-a-1100479.html (zuletzt besucht am: 16. 12. 2016).

[The] The GnuPG Authors. *openpgpdefs.h of GnuPG Source*. URL: http://git.gnupg.org/cgi-bin/gitweb.cgi?p=gnupg.git;a=blob;f=common/openpgpdefs.h;h=e200d6b3bf2b836dc7f3fa4e52991b2322456feb;hb=24e0f1d56e6f56e7fb52b5c6bdb100131e12dfe3#l88 (zuletzt besucht am: 01. 12. 2016).

[Ulr+11] Alexander Ulrich u. a. „Investigating the OpenPGP Web of Trust“. In: *Computer Security – ESORICS 2011: 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12-14,2011. Proceedings*. Hrsg. von Vijay Atluri und Claudia Diaz. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, S. 489–507. ISBN: 978-3-642-23822-2. DOI: 10.1007/978-3-642-23822-2_27. URL: http://dx.doi.org/10.1007/978-3-642-23822-2_27.

[Wal] Daniel Walker. URL: https://commons.wikimedia.org/wiki/File%3ASix_degrees_of_separation.svg (zuletzt besucht am: 16. 12. 2016).

[Way] Peter Wayner. *Germany Awards Grant for Encryption*. URL: http://partners.nytimes.com/library/tech/99/11/cyber/articles/19encrypt.html (zuletzt besucht am: 16. 12. 2016).

[Yua+11] Weiwei Yuan u. a. „The small-world trust network“. In: *Applied Intelligence* 35.3 (2011), S. 399–410. ISSN: 1573-7497. DOI: 10.1007/s10489-010-0230-7. URL: http://dx.doi.org/10.1007/s10489-010-0230-7.